

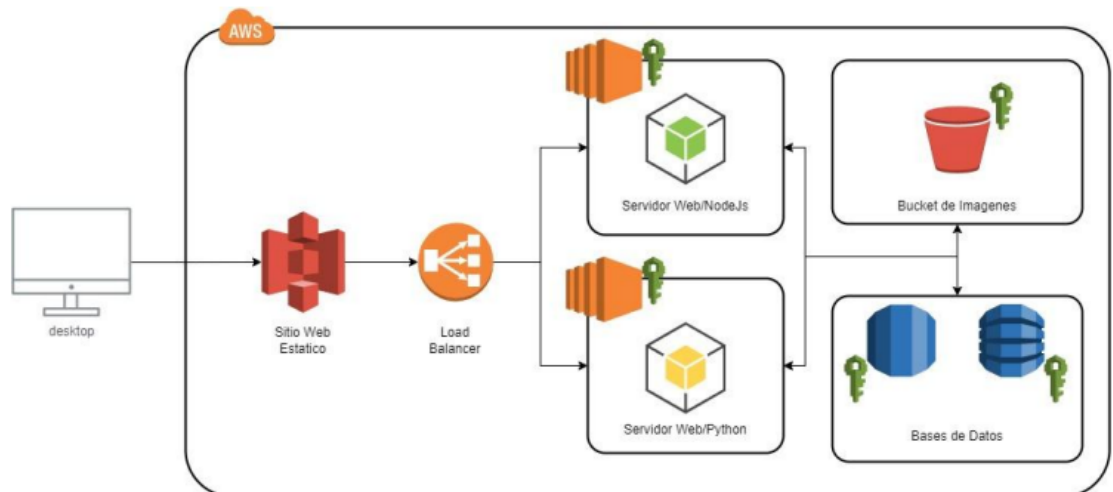
MANUAL TÉCNICO

- **Objetivos**

- El objetivo de este manual es dar un panorama general de los servicios ofrecidos por AWS (Amazon Web Services) y la forma en que se pueden implementar para crear un sitio web estático el cual se encarga de generar peticiones que pasan por un Load Balancer.
- Entender cómo implementar un Bucket de imágenes en AWS
- Conocer la correcta implementación de instancias EC2 para levantar Api's
- Entender la arquitectura que se implementó en este caso, la cual consta de un sitio web estático, load balancer, 2 api's, un bucket de imágenes y una base de datos en PostgreSQL usando RDS

- **Arquitectura**

La arquitectura utilizada es la siguiente:



En esta arquitectura se utilizaron 2 maquinas virtuales para poder utilizar dos Api's diferentes, una en Nodejs y otra en Python, las cuales tenían comunicación con un bucket de imágenes y la base de datos implementada con RDS, el usuario tiene comunicación con estas apis por medio de un frontend el cual se desarrolló en ReactJs, este frontend fue puesto en un sitio web estático y genera peticiones que pasan por un load balancer el cual decide si se utiliza la api de python o la de nodejs, todo esto utiliza servicios de aws.

- **Usuarios de IAM y Políticas asociadas**

Estos son los usuarios utilizados para este proyecto:

Nombre de usuario ▼	Grupos ▼	Última activ... ▼	MFA ▼
Administrador_201503958	Ninguno	✓ hace 12 minutos	Ninguno
DamC	Proyecto1	✓ hace 9 horas	Ninguno
grupo2-base	base-g2	✓ hace 2 minutos	Ninguno

- **Administrador_201503958:**

Este es el encargado de dar permisos a los demás usuarios para que puedan utilizar cualquier recurso de aws en específico.

También se encargó de crear el load balancer y el sitio web estático.

- **DamC:**

Este usuario se encargó de crear las máquinas virtuales y el bucket para poder tener las 2 apis en ellas.

- **grupo2-base:**

Este usuario solamente tiene permiso de manejar la base de datos utilizada.

- **Configuración del servicio**

- **EC2:**

Para la creación de una nueva vm se necesita colocar un nombre a la instancia, luego se selecciona un sistema operativo y por último se seleccionan las casillas para poder permitir el tráfico http y https.

EC2 > Instancias > Lanzar una instancia

Lanzar una instancia [Información](#)

Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

Nombre y etiquetas [Información](#)

Nombre

[Agregar etiquetas adicionales](#)

▼ Imágenes de aplicaciones y sistemas operativos (Amazon Machine Image) [Información](#)

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Recientes **Inicio rápido**

Amazon

macOS

Ubuntu

Windows

Red Hat

S

Recientes

Inicio rápido

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

S

Buscar más AMI

Incluidas las AMI de AWS, Marketplace y la comunidad

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

Apto para la capa gratuita

ami-05fa00d4c63e32376 (64 bits (x86)) / ami-05f3141013eebdc12 (64 bits (Arm))

Virtualización: hvm Habilitado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220805.0 x86_64 HVM gp2

Arquitectura

ID de AMI

64 bits (x86)

ami-05fa00d4c63e32376

Proveedor verificado

Firewall (grupos de seguridad)

Información

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☒ Crear grupo de seguridad

☐ Seleccionar un grupo de seguridad existente

Crearemos un nuevo grupo de seguridad denominado "launch-wizard-3" con las siguientes reglas:

☒ Permitir el tráfico de SSH desde

Ayuda a establecer conexión con la instancia

Cualquier lugar
0.0.0.0/0

☐ Permitir el tráfico de HTTPs desde Internet

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

☐ Permitir el tráfico de HTTP desde Internet

Para configurar un punto de enlace, por ejemplo, al crear un servidor web

⚠ Las reglas con la fuente 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia.

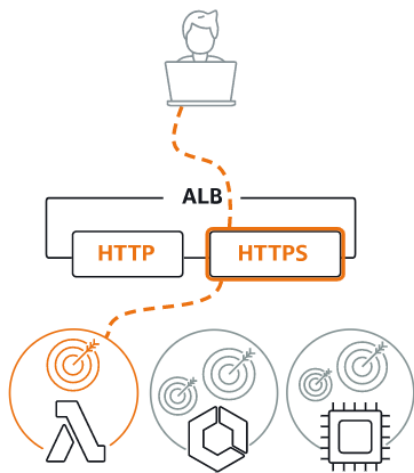
Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

✕

Después de crear la instancia se deben configurar los puertos que se utilizaran, en este caso es el puerto 3000 en las opciones de seguridad de la vpc.

Reglas de entrada <small>Información</small>							
ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>		
sgr-071aeb1172db88ff	HTTP	TCP	80	Person...	Q	0.0.0.0/0	Eliminar
sgr-0105a5f1d8c7e5c93	SSH	TCP	22	Person...	Q	0.0.0.0/0	Eliminar
sgr-05ee589b43c972488	HTTPS	TCP	443	Person...	Q	0.0.0.0/0	Eliminar
sgr-03abfa4e494426521	TCP personalizado	TCP	3000	Person...	Q	0.0.0.0/0	Eliminar
Agregar regla							

- **Load Balancer:**
Se selecciona esta opción para poder utilizar el load balancer:
Application Load Balancer Info



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Se coloca un nombre al load balancer que se utilizara y se deben seleccionar más de dos regiones, una de estas debe ser la misma donde están alojadas las instancias con las que se desea conectar el load balancer se deben seleccionar también los grupos de seguridad que tienen las dos instancias y se debe generar un nuevo grupo para el load balancer.

Basic configuration

Load balancer name

Name must be unique within your AWS account and cannot be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme

Info

Scheme cannot be changed after the load balancer is created.

☒ Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ Internal

An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type

Info

Select the type of IP addresses that your subnets use.

☒ IPv4

Recommended for internal load balancers.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

Network mapping

Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC

Info

Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-

vpc-0cfc428b03c686f19

IPv4: 172.31.0.0/16

Mappings

Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☐ us-east-1a

☐ us-east-1b

☐ us-east-1c

☐ us-east-1d

☐ us-east-1e

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

Select up to 5 security groups

[Create new security group](#)

default sg-02e5fc5ea173ff825 X

VPC: vpc-0cfc428b03c686f19

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Remove

Protocol

Port

HTTP

:

80

1-65535

Default action

[Info](#)

Forward to

Select a target group

Se deben seleccionar las instancias a las cuales enviará datos este servicio y en qué puerto lo hará.

Details

arn:aws:elasticloadbalancing:us-east-1:865263502849:targetgroup/grupo2-semi1/a6f5dba849b05f37

Target type

Instance

IP address type

IPv4

Protocol : Port

HTTP: 80

Load balancer

semi1-g2

Protocol version

HTTP1

VPC

vpc-0cfc428b03c686f19

Total targets

2

Healthy

2

Unhealthy

0

Unused

0

Initial

0

Draining

0

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2)

Filter resources by property or value

< 1 >

☐

Instance ID

Name

Port

Zone

Health status

Health status details

☐

i-Oe30d388500f17011

api-python

3000

us-east-1c

healthy

☐

i-062d941a2cbfd83f9

api-node

3000

us-east-1c

healthy

Tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration [Edit](#)

Load balancer name not defined

Internet-facing

IPv4

Security groups [Edit](#)

default sg-02e5fc5ea173ff825

Network mapping [Edit](#)

VPC vpc-0cfc428b03c686f19

Subnet not defined

Listeners and routing [Edit](#)

HTTP:80 defaults to Target group not defined

Add-on services [Edit](#)

None

Tags [Edit](#)

None

Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Cancel

Create load balancer

- **Bucket:**

Para la creación de un bucket solo se debe colocar un nombre, una región y desmarcar las opciones de bloqueo de acceso público.

Crear bucket Info

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

Configuración general

Nombre del bucket

El nombre del bucket debe ser único en todo el mundo y no debe contener espacios ni letras mayúsculas. [Consulte las reglas para la denominación de los buckets](#)

Región de AWS

EE. UU. Este (Norte de Virginia) us-east-1

Copiar la configuración del bucket existente: *opcional*
Solo se copia la configuración del bucket en los siguientes ajustes.

Elegir el bucket

Propiedad de objetos Info

Controle la propiedad de los objetos escritos en este bucket desde otras cuentas de AWS y el uso de listas de control de acceso (ACL). La propiedad de los objetos determina quién puede especificar el acceso a los objetos.

☒ **ACL deshabilitadas (recomendado)**
Todos los objetos de este bucket son propiedad de esta cuenta. El acceso a este bucket y sus objetos se especifica solo mediante políticas.

☐ **ACL habilitadas**
Los objetos de este bucket pueden ser propiedad de otras cuentas de AWS. El acceso a este bucket y sus objetos se puede especificar mediante ACL.

Propiedad del objeto

Aplicada al propietario del bucket

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)

☐ **Bloquear todo el acceso público**
Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

☐ **Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)**
S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.

En la parte de permisos, política del bucket, se debe colocar el siguiente json para que tenga un acceso público este bucket.

Política de bucket
La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

Editar

Eliminar

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::appweb-grupo2-p1/"
    }
  ]
}
```

Copiar

- **Web estática:**

Para la creación de la web estática se debe crear un build en la aplicación que se utilizara, en este caso que se utilizó una aplicación en react se utiliza el comando `npm run build` y esta carpeta es la que se subirá al bucket creado para la web estática, luego se habilitará la opción de web estática que está en propiedades, en la opción final.

Alojamiento de sitios web estáticos

Editar

Utilice este bucket para alojar un sitio web o redirigir solicitudes. [Más información](#)

Alojamiento de sitios web estáticos

Habilitada

Tipo de alojamiento

Alojamiento de buckets

Punto de enlace de sitio web del bucket

Al configurar su bucket como sitio web estático, el sitio web estará disponible en el punto de enlace del sitio web específico de la región de AWS del bucket. [Más información](#)

http://front-semi1.s3-website-us-east-1.amazonaws.com

Se colocará el como documento de índice nuestro `index.html`.

Documento de índice

Especifique la página predeterminada o de inicio del sitio web.

`index.html`

Documento de error - *opcional*

Esto se devuelve cuando se produce un error.


`index.html`


- **Base de datos:**


Se selecciona el motor de bases de datos que se utilizara y la version que se utilizara.


Opciones del motor


Tipo de motor [Información](#)


☐ Amazon Aurora


☒ MySQL



☐ MariaDB


☐ PostgreSQL


☐ Oracle


☐ Microsoft SQL Server


Edición
☒ Comunidad de MySQL

 **Problemas/Limitaciones conocidas**
Revise [Problemas/limitaciones conocidas](#) para obtener más información sobre problemas potenciales de compatibilidad con versiones de base de datos específicas.

Versión
MySQL 8.0.28

Se coloca una contraseña.

Configuración

Identificador de instancias de bases de datos [Información](#)

Escriba un nombre para la instancia de base de datos. El nombre debe ser único en relación con todas las instancias de base de datos pertenecientes a su cuenta de AWS en la región de AWS actual.

database-2

El identificador de la instancia de base de datos no distingue entre mayúsculas y minúsculas, pero se almacena con todas las letras en minúsculas (como en "miinstanciadebd"). Restricciones: de 1 a 60 caracteres alfanuméricos o guiones. El primer carácter debe ser una letra. No puede contener dos guiones consecutivos. No puede terminar con un guion.

▼ Configuración de credenciales

Nombre de usuario maestro [Información](#)

Escriba un ID de inicio de sesión para el usuario maestro de la instancia de base de datos.

admin

De 1 a 16 caracteres alfanuméricos. El primer carácter debe ser una letra.

☐ Generación automática de contraseña
Amazon RDS puede generar una contraseña en su nombre, o bien puede especificar su propia contraseña.

Contraseña maestra [Información](#)

Restricciones: debe tener al menos 8 caracteres ASCII imprimibles. No puede contener ninguno de los siguientes caracteres: / (barra diagonal), ' (comillas simples), " (dobles comillas) y @ (signo de arroba).

Confirmar contraseña [Información](#)

- **Conclusiones**

- Los servicios que AWS ofrece son capaces de permitir la implementación de arquitecturas de software las cuales cumplen con requisitos rigurosos como políticas de seguridad para usuarios IAM de un mismo proyecto, lo cual es bastante útil para asegurar software de calidad asignando roles de trabajo en un equipo.
- Este proyecto permitió comprender cómo funciona un bucket, el cual se encarga de contener objetos
- A través de diferentes servicios de AWS se pudo implementar un sitio web estático desarrollado en ReactJs el cual fue capaz de generar peticiones que pasaban por un load balancer y así almacenar información en una base de datos e imágenes en un bucket implementado en S3.